

## CRYPTOGRAPHY WITH RIGHT-ANGLED ARTIN GROUPS

RAMÓN FLORES AND DELARAM KAHROBAEI

**ABSTRACT.** In this paper we propose right-angled Artin groups as platform for a secret sharing scheme based on the efficiency (linear time) of the word problem. We define two new problems: subgroup isomorphism problem for Artin subgroups and group homomorphism problem in right-angled Artin groups. We show that the group homomorphism and graph homomorphism problems are equivalent, and the later is known to be NP-complete. We propose two authentication schemes based on subgroup isomorphism problem and group homomorphism problem in right-angled Artin groups. In the case of subgroup isomorphism problem, we bring some results due to Bridson who shows there are right-angled Artin groups in which this problem is unsolvable. Note that our schemes are similar to what Grigoriev and Shpilrain proposed for graphs.

## CONTENTS

1. Introduction	1
2. Secret sharing threshold schemes	2
3. Authentication Schemes Based on the Group Homomorphism and the Subgroup Isomorphism problems	2
3.1. An Authentication scheme using Group Homomorphism problem	3
3.2. An Authentication Scheme Based on the Subgroup Isomorphism problem	3
4. Right Angled Artin Groups	3
4.1. Definition and Presentation	3
4.2. The complexity of algorithmic problems	5
Acknowledgements	6
References	6

## 1. INTRODUCTION

The note is motivated by the fact that right-angled Artin groups can be thought as graphs and many graph-theoretic problems that are proved to be NP-complete can be translated to a group-theoretic setting in the right-angled Artin groups. Besides the fact that is always of interest to introduce new applications of the group theory in cryptography, we also note that working with group presentation is easier and sometimes more practical that working with graphs.

We note that Shpilrain and Zapata have proposed a key exchange based on Artin groups but this class is much bigger than right-angled Artin groups [16].

## 2. SECRET SHARING THRESHOLD SCHEMES

Habeb, Kahrobaei, Shpilrain have proposed a cryptosystem based on efficiency of the word problem [9], and we intend to use it with right-angled Artin groups. The system is based on two schemes.

In the first protocol, which is an  $(n, n)$ -threshold scheme, the dealer distributes a

$k$ -column  $C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{pmatrix}$  consisting of 0's and 1's among  $n$  participants in such a way

that the vector can be retrieved only when all  $n$  participants cooperate. Then the dealer splits the secret bit column  $C$  (the actual secret to be shared) into a mod 2

sum  $C = \sum_{j=1}^n C_j$  of  $n$  bit columns, and the participant  $P_i$  can only retrieve the actual

values of the column  $C_i$  if he/she is able to solve the word problem in a certain group  $G_i$  of the family whose set of generators is public (and the same for all the participants), but whose relations  $R_i$  are only known for him/her. Moreover, the participants can use secure computation of a sum as proposed in [7] if they do not want to reveal their individual column vectors, and therefore their individual secret shares, to each other. Moreover, we note that the dealer can efficiently build a word  $w$  in the normal closure of  $R_i$  as a product of arbitrary conjugates of elements of  $R_i$ , so that  $w = 1$  in the corresponding group  $G_i$ .

The second protocol is a  $(t, n)$ -threshold scheme, and a modification of the previous one that takes into account some ideas from [15], and allows a subset of size  $t$  of the total number of participants  $n$  to reconstruct all the information. Now the secret is an element  $x \in \mathbb{Z}_p$ , and the dealer chooses a polynomial  $f$  of degree  $t - 1$  such that  $f(0) = x$ . In addition the dealer determines integers  $y_i = f(i) \pmod{p}$  that are distributed to participants  $P_i$ ,  $1 \leq i \leq n$  (we assume that all integers  $x$  and  $y_i$  can be written as  $k$ -bit columns). A set of group generators  $\{x_1, \dots, x_m\}$  is made public, and every participant  $P_j$  receives through a secure channel a set of relators  $R_j$ . Then the dealer distributes over open channels  $k$ -columns

$b_j = \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{kj} \end{pmatrix}$ ,  $1 \leq j \leq n$ , of words in  $x_1, \dots, x_m$  to each participant  $P_j$ , that can

retrieve from its column its correspondent  $y_j$  by solving the word problem in the group defined by the set of generators and the relators  $R_j$ . Finally, every subset of  $t$  participants can recover the secret  $x$  by constructing the polynomial  $f$  via interpolation, and this scheme can be arranged in such a way that participants do not have to reveal their individual shares  $y_i$  to each other if they do not want to. More details of these protocols can be found in [9].

## 3. AUTHENTICATION SCHEMES BASED ON THE GROUP HOMOMORPHISM AND THE SUBGROUP ISOMORPHISM PROBLEMS

Grigoriev and Shpilrain have proposed in [8] some authentication protocols using graph homomorphisms problem and subgraph isomorphism problem. In the sequel, we introduce two different protocols, which are based on the group homomorphism and the subgroup isomorphism problems, and that we introduce using right-angled Artin groups as a platform; they are inspired by the work of these authors in the sense that they are originally (but not necessarily) addressed to be used with group

graphs as a platform. In this sense, and as we will see below, we would make profit of unsolvability results for groups and also for graphs. We remark that we have developed no analogy of the protocol based in the classical Graph Isomorphism problem, as it has recently been shown by Babai [1] that its complexity is quasi-polynomial.

### 3.1. An Authentication scheme using Group Homomorphism problem.

Consider two finitely presented groups  $G_1 = \langle S_1 | R_1 \rangle$  and  $G_2 = \langle S_2 | R_2 \rangle$ , being  $S_i$  generators and  $R_i$  relations,  $i = 1, 2$ . The Group Homomorphism problem asks if there is a homomorphism  $G_1 \rightarrow G_2$  that takes generators in  $S_1$  to generators in  $S_2$ .

The authentication protocol is the following:

- (1) Alice's public key consists of two finitely presented groups  $G_1 = \langle S_1 | R_1 \rangle$  and  $G_2 = \langle S_2 | R_2 \rangle$ . Alice's long term private key is a homomorphism  $\alpha$  sending generators in  $S_1$  to generators in  $S_2$ .
- (2) Alice selects another finitely presented group  $G = \langle S | R \rangle$ , and a homomorphism  $\beta : G \rightarrow G_1$  which sends generators in  $S$  to generators in  $S_1$ . Then she sends  $G = \langle S | R \rangle$  to Bob, and keeps the homomorphism  $\beta$  to herself.
- (3) Bob chooses a random bit and sends  $c$  to Alice.
  - When  $c = 0$ , Alice sends the homomorphism  $\beta$  to Bob, and Bob should check if  $\beta(G) = G_1$ , and if  $\beta$  is a homomorphism that takes generators in  $S$  to generators in  $S_1$ .
  - When  $c = 1$ , Alice sends the composite  $\alpha\beta$  to Bob, and Bob checks whether  $\alpha\beta(G) = G_2$ , and if the composite is a homomorphism that takes generators in  $S$  to generators in  $S_2$ .

### 3.2. An Authentication Scheme Based on the Subgroup Isomorphism problem.

The authentication protocol we propose is as follows:

- (1) Alice's public key consists of two isomorphic subgroup of group  $\Gamma$ ,  $G_1$  and  $G_2$ . Alice's long-term private key is an isomorphism  $\alpha : G_1 \rightarrow G_2$ .
- (2) To begin authentication, Alice selects a group  $G$  together with the isomorphism  $\beta : G \rightarrow G_1$  and sends the group  $G$  (the commitment) to Bob, while keeping  $\beta$  to herself.
- (3) Bob chooses a random bit  $c$  and sends it to Alice.
  - If  $c = 0$ , then Alice sends the isomorphism  $\beta$  to Bob, and Bob checks whether  $\beta(G) = G_1$  and whether  $\beta$  is an isomorphism.
  - If  $c = 1$ , then Alice sends the composition  $\alpha\beta = \beta(\alpha)$  to Bob, and Bob checks whether  $\alpha\beta(G) = G_2$  and whether  $\alpha\beta$  is an isomorphism.

## 4. RIGHT ANGLED ARTIN GROUPS

Here we introduce the main facts concerning right-angled Artin groups, a class introduced by Baudisch at the end of the seventies. Good surveys about the topic can be found in [12] and [4].

### 4.1. Definition and Presentation.

**Definition 4.1** (Right-angled Artin groups). *Let  $\Gamma$  denote a finite simplicial graph. We will write  $V = V(\Gamma)$  for the finite set of vertices and  $E(\Gamma) \subset V \times V$  for the set of edges, viewed as unordered pairs of vertices. The requirement that  $\Gamma$  be simplicial*

simply means that the diagonal of  $V \times V$  is excluded from the set of edges. The right-angled Artin group on  $\Gamma$  is the group

$$A(\Gamma) = \langle V \mid [v_i, v_j] = 1 \text{ whenever } (v_i, v_j) \in E \rangle.$$

In other words,  $A(\Gamma)$  is generated by the vertices of  $\Gamma$ , and the only relations are given by commutation of adjacent vertices.

Observe that right-angled Artin groups, that are associated to a finite simplicial graph (the *Artin graph*), are always finitely presented. It is clear from the definition that there is a bijective correspondence between isomorphism types of right-angled Artin groups and isomorphism types of finite simplicial graphs, in the sense that two right-angled Artin groups  $A(\Gamma)$  and  $A(\Lambda)$  are isomorphic if and only if  $\Gamma = \Lambda$ . Moreover, a map  $f : A_1 \rightarrow A_2$  of right-angled Artin groups is a homomorphism if and only if it induces a graph homomorphism between the corresponding graphs.

It is also apparent that the right-angled Artin group corresponding to the empty graph in  $n$  vertices is the free group  $F_n$ , while the corresponding to the complete graph is the free abelian group  $\mathbb{Z}^n$ . Moreover, if  $A$  is a right-angled Artin group in  $n$  generators, there always exist surjections  $F_n \twoheadrightarrow A \twoheadrightarrow \mathbb{Z}^n$ . So in some sense, these groups represent a “hierarchy” between free groups and abelian groups.

There are several interesting families of subgroups of right-angled Artin groups, for example surface groups, graph braid groups and Bestvina-Brady group. We will be specially interested in the subgroups generated by subsets of the set  $S$  of generators. If  $T \subset S$  is such a subgroup of a right-angled Artin groups  $A$ , it is usually denoted by  $A_T$  and called a *special subgroup* of  $A$ . Note that every special subgroup of  $A$  gives rise to a subgraph of  $\Gamma_A$ , but the converse is not true. For example, if we consider the graph with vertices  $\{v_0, v_1\}$  and edge  $[v_0, v_1]$ , which corresponds to the free abelian group in two generators, the 0-dimensional subgraph defined by the two vertices produces the free group in two generators, which is not a subgroup of  $\mathbb{Z}^2$ . It is easy to see that a subgraph  $\Gamma'$  of an Artin graph  $\Gamma$  defines a special subgroup of the corresponding right-angled Artin groups if and only if  $\Gamma'$  is a *full* subgraph of  $\Gamma$ .

**Definition 4.2.** A subgraph  $\Gamma'$  of a graph  $\Gamma$  is full if for every pair of vertices  $\{v, w\}$  in  $\Gamma'$  such that  $[v, w]$  is an edge in  $\Gamma$ ,  $[v, w]$  is an edge in  $\Gamma'$ .

The full subgraphs are also called spanning or induced. This condition is important in order to use these subgroups as a platform for authentication.

Right-angled Artin groups are examples of a more general class of groups:

**Definition 4.3.** Consider a word  $w(a, b)$  in two letters. Given a finite simplicial graph  $\Gamma = (V, E)$ , we can define a verbal group  $G(\Gamma)$ , where the generators are given by the vertices and there is an edge  $[v_i, v_j]$  if and only if  $w(v_i, v_j) = 1$ .

For all these groups there is an equivalence between their isomorphism types and the isomorphism types of finite simplicial graphs, and in particular the right-angled Artin groups correspond to the particular case in which  $w$  is the commutator. This class of groups contains in fact non-Artin groups and non-right-angled Artin groups. However, in order to construct a class like this containing all Artin groups, multi-graphs (and the corresponding associated Isomorphism/Homomorphism problems) should be considered. We concentrate in the right-angled Artin case because for them we know how to prove the appropriate complexity results (see next section and Remark 4.4).

**4.2. The complexity of algorithmic problems.** In this section we state the complexity results that make right-angled Artin groups a good platform for the previous protocols.

**4.2.1. Word problem.** To introduce a family of groups as a platform for the secret sharing scheme described [9] it is necessary that its word problem can be solved efficiently. In the mentioned paper, for example, the authors apply their cryptosystem for small cancellation groups. In the case of right-angled Artin groups, the easiness of the word problem was first proved in a paper by Liu-Wrathall-Zeger [13] which in a more general framework of free partially commutative monoids, describes an algorithm which is effective in linear polynomial time. More recently, Crisp-Goddelle-Wiest [5] have extended this result (with different methods) to some families of subgroups of right-angled Artin groups, as for example braid groups.

**4.2.2. Group problems and complexity.** The security of our proposed authentication schemes relies on the difficulty of the Group Homomorphism problem and the Subgroup Isomorphism problem for the chosen groups. For the former, observe that the problem is equivalent to the Graph Homomorphism problem for graphs, as there is a bijection between right-angled Artin groups and finite simplicial graphs, and recall that this problem has been shown to remain NP-complete even when the graph in the right is a triangle [6]. Hence, it would be enough here to select two right-angled Artin groups  $\Gamma_1$  and  $\Gamma_2$  such that  $\Gamma_2$  contains a free abelian group in three generators.

Concerning the Subgroup Isomorphism problem, M. Bridson has proved [2] that there exist families of right-angled Artin groups for which this problem is unsolvable, even for finitely presented subgroups. Let us briefly recall the construction. He starts with a free group in a finite number of generators, and performs over it Rips construction [14] in the specific version of Haglund and Wise ([10], Section 10). In this way we obtain an explicit presentation of a hyperbolic group  $\Gamma$  that possess a finite index subgroup  $\Gamma_0 < \Gamma$ , which is the fundamental group of a special cube complex. This complex is subject to certain restrictions ([10], Theorem 1.1), that give rise to the existence of a local isometry with a standard cube complex, and in particular imply the existence of an embedding of  $\Gamma_0$  in the fundamental group of the latter, which is a right-angled Artin group and we call  $A$ . The group  $\Gamma_0$  also projects onto a non-abelian free group, and the kernel is infinite and finitely-generated. Then, by a previous result of Bridson-Miller [3], the subgroup Isomorphism problem is unsolvable for every product  $\Gamma_0 \times \Gamma_0 \times F$ , being  $F$  any non-abelian free group. As  $\Gamma_0 < A$ , the problem is also unsolvable for  $A \times A \times F$ , and this is a right-angled Artin group itself, as it is the product of right-angled Artin groups.

In general, to compare the Subgroup Isomorphism problem and the Subgraph Isomorphism problem we need that the generators and relators on the groups can be represented as a graph. But this is only a necessary condition. For example, in right-angled Artin groups there are plenty of subgroups that cannot be represented by a subgraph of the Artin graph (for example, the cyclic group generated by the product of two generators). An authentication scheme based in this problem for right-angled Artin groups only should make use of the special subgroups, and should take into account the fact that not every subgraph of the Artin graph represents a special subgroup. This approach is closer to the problem of subgroup isomorphism

for full subgraphs of a finite graph, usually called the *induced Subgraph Isomorphism problem*, which is known to be NP-complete in general (see [11] for a reference). For the classical Subgroup Isomorphism problem, it is more straightforward to appeal to Bridson unsolvability results described above.

**Remark 4.4.** *Families of verbal groups in the sense of Definition 4.3 are potential examples of new platforms for the above protocols, provided complexity results for the Homomorphism and Subgroup Isomorphism problems are available for them.*

#### ACKNOWLEDGEMENTS

Delaram Kahrobaei is partially supported by a PSC-CUNY grant from the CUNY Research Foundation, the City Tech Foundation, and ONR (Office of Naval Research) grant N00014-15-1-2164. Part of the work was done while visiting the UPV/EHU funded by the ERC grant PCG-336983. Delaram Kahrobaei has also partially supported by an NSF travel grant CCF-1564968 to IHP in Paris. Ramón Flores is partially supported by MEC grant MTM2010-20692.

#### REFERENCES

- [1] L. Babai. Graph isomorphism in quasipolynomial time. *arXiv preprint arXiv:1512.03547*, 2015.
- [2] M. Bridson. Cube complexes, subgroups of mapping class groups, and nilpotent genus. *Geometric group theory, IAS/Park City Math. Ser.*, 21(21), 2014.
- [3] M. Bridson and C. Miller. Recognition of subgroups of direct products of hyperbolic groups. *Proc. Amer. Math. Soc.*, 132:59–65, 2003.
- [4] R. Charney. An introduction to right-angled artin groups. *Geom. Dedicata*, 125:141–158, 2007.
- [5] J. Crisp, E. Godelle, and B. Wiest. A linear time solution to the conjugacy problem in right-angled artin groups and their subgroups. *Journal of Topology*, 2:442–460, 2009.
- [6] M. Garey and J. Johnson. *Computers and Intractability, A Guide to NP-Completeness*. W. H. Freeman, 1979.
- [7] D. Grigoriev and V. Shpilrain. Unconditionally secure multiparty computation and secret sharing. *preprint*.
- [8] D. Grigoriev and V. Shpilrain. Authentication schemes from actions on graphs, groups, or rings. *Ann. Pure Appl. Logic*, 162:194–200, 2010.
- [9] M. Habeeb, D. Kahrobaei, and V. Shpilrain. A secret sharing scheme based on group presentations and the word problem. *Contemp. Math., Amer. Math. Soc.*, 582:143–150, 2012.
- [10] F. Haglund and D. Wise. Special cube complexes. *Geom. Funct. Anal.*, 17:1551–1620, 2008.
- [11] H. Kijima, Y. Otachi, T. Saitoh, and T. Uno. Subgraph isomorphism in graph classes. *Discrete Mathematics*, 312:3164–3173, 2012.
- [12] T. Korbeda. Right-angled artin groups and their subgroups. *Lecture notes Yale University*, pages 1–50, 2013.
- [13] H. Liu, C. Wrathall, and K. Zeger. Efficient solution of some problems in free partially commutative monoids. *Information and Computation*, 89:180–198, 1990.
- [14] E. Rips. Subgroups of small cancellation groups. *Bull. London Math. Soc.*, pages 45–47, 1982.
- [15] A. Shamir. How to share a secret. *Comm. ACM*, 22:612–613, 1979.
- [16] V. Shpilrain and G. Zapata. Combinatorial group theory and public key cryptography. *Applicable Algebra in Engineering, Communication and Computing*, 17:291–302, 2006.

RAMÓN FLORES, DEPARTMENT OF GEOMETRY AND TOPOLOGY, UNIVERSITY OF SEVILLE, SPAIN  
E-mail address: `ramonjflores@us.es`

DELARAM KAHROBAEI, CUNY GRADUATE CENTER, PHD PROGRAM IN COMPUTER SCIENCE  
AND NYCCT, MATHEMATICS DEPARTMENT, CITY UNIVERSITY OF NEW YORK  
E-mail address: `dkahrobaei@gc.cuny.edu`